PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	)
	)
Barton et al.	) Art Unit: 2137
	)
Application No. 09/916,600	) Examiner: Pyzocha, Michael J.
	)
Filed: 07/26/2001	) Date: 03/29/2007
	)
For: SYSTEM, METHOD AND COMPUTER PROGRAM PRODUCT FOR ANTI-VIRUS SCANNING IN A STORAGE SUBSYSTEM	)
	)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

ATTENTION: Board of Patent Appeals and Interferences

REPLY BRIEF (37 C.F.R. § 41.37)

This Reply Brief is being filed within two (2) months of the mailing of the Examiner's Answer mailed on 01/29/2007.

Following is an issue-by-issue reply to the Examiner's Answer.

The claims of the groups noted below do not stand or fall together. In the present section, appellant explains why the claims of each group are believed to be separately patentable.

Issue #1:

The Examiner has rejected Claim 42 under 35 U.S.C. 112, first paragraph, as providing new matter not originally described in the Specification.

Group #1: Claims 42 and 43

In the Examiner's Answer mailed 01/29/2007, the Examiner has withdrawn the rejection under 35 U.S.C. 112, first paragraph.

Issue #2:

The Examiner has rejected Claims 1-40 under 35 U.S.C. 103(a) as being unpatentable over Makita, U.S. Patent No. 2001/0007120, in view of Flint, U.S. Patent No. 6,735,700.

Group #1: Claims 1, 2, 4, 5, 10, 11, 15-17, 18, 20, 21, 26, 27, 31-34 and 39

With respect to Claim 1, the Examiner continues to rely on the following excerpt from Flint to meet appellant's claimed "wherein a user is allowed to disable the scanning module, and data is precluded from being transmitted from the storage to the central processing unit upon the disabling of the scanning module."

> "The third activity waits for user input (block 421). When user input is received, it is evaluated to determine if the user has requested that a particular file be scanned (block 423). If so, an on-demand scan is performed using the requested file as the scan set as described below with reference to FIG. 6. **If the user input specifies the termination of the anti-virus program (block 427), a termination process illustrated by block 429 and described in more detail below in conjunction with FIG. 8 is performed.** When the user has previously requested the scanning facility be stopped (as described next), the user can request it be restarted (block 431). Any other user input, including a request to stop the scanning facility, is processed at block 433. Such user input also includes changing preference parameters that control the overall functioning of the anti-virus software. The

> user can also specify which files to include in a pre-defined scan set that is used by the on-demand scan of FIG. 6. The handling of such user input is well understood in the art and is not discussed further. Moreover, it will be appreciated that the input interface is conventional and thus not illustrated." (Col. 9, lines 5-24 - emphasis added)

Appellant respectfully asserts that the above excerpt from Flint simply discloses "[i]f the user input specifies the termination of the anti-virus program (block 427), a termination process illustrated by block 429 and described in more detail below in conjunction with FIG. 8 is performed". Thus, Flint only teaches a user terminating the anti-virus program, and not "data is precluded from being transmitted from the storage to the central processing unit upon the disabling of the scanning module," as claimed by appellant.

To further clarify this distinction, appellant respectfully points out Fig. 8 in Flint, as referred to in the above excerpt. Specifically, Fig. 8 teaches writing to permanent storage (block 803) even after a user has specified to terminate the anti-virus program (block 429 of Fig. 4). Appellant respectfully asserts that this clearly *teaches away* from appellant's claim language since appellant specifically claims "data is precluded from being transmitted from the storage to the central processing unit upon the disabling of the scanning module" (emphasis added), as claimed. Allowing the data to be written to storage or read from storage without fully completing a scan, as in Flint, would provide the opportunity for malicious code to execute and/or proliferate on the systems sought to be protected. Appellant's claimed invention is clearly capable of avoiding such a situation.

In the Advisory Action dated 05/16/2005, the Examiner has argued that Makita, in combination with Flint, teaches appellant's claim language. Specifically, the Examiner has argued that Makita teaches "[t]he storage location retrieves the data and performs an internal virus check on the data before it sends the data back to the cpu (host) ([0180]-[0184])." Additionally, the Examiner has argued that Flint teaches the idea of a user being able to disable and enable a virus scanning module (Col. 9, lines 5-24). From this, the Examiner has concluded that the combination of such teachings meet appellant's claimed method "wherein a user is allowed to disable the scanning module, and data is precluded from being transmitted from the storage to the central processing unit upon the disabling of the scanning module."

Appellant respectfully disagrees. Makita merely teaches two scenarios. First, if a virus is found during the virus check, transmission to the host is stopped ([00183]). Second, if a virus is not found during the virus check, the information is transmitted to the host ([00184]). Clearly, there is no disclosure of the result when no virus check is performed, since Makita does not allow for this option. Thus, only appellant teaches and claims that "data is precluded from being transmitted from the storage to the central processing unit upon the disabling of the scanning module."

In the Examiner's Answer mailed 01/29/2007, the Examiner has argued that "Flint teaches disabling a virus scanner (see column 9 lines 10-15), when the virus scanner is stopped (i.e. disabled) the session stamp of the file is invalidated (see column 9 lines 3-4)." Further, the Examiner has argued that "referring to figure 6, number 611, the session stamp is checked to determine whether it is valid or not, when it is not, the file is scanned for viruses and the session stamp is updated, since the virus scanner is stopped at this point the session stamp is updated to state that it is still invalid as described in column 9 lines 3-4." Additionally, the Examiner has argued that "figure 8, which related to the specifics of when the virus scanner is terminated, the virus scanning program and method is stopped without updating the session stamp to be valid therefore when attempting to access this file the above steps will be repeated as long as the virus scanner is off so the session stamp will never be validated and therefore the file cannot be accessed as further described with respect to figure 7 and column 10 lines 20-32."

Appellant respectfully disagrees with the Examiner's arguments, and asserts that Flint discloses that "an option is provided in an alternate embodiment that allows the user to only stop the scanning facility of program 305" where, "[i]n this embodiment, the program 305 continues to monitor all relevant file system accesses" (Col. 7, lines 57-61 – emphasis added). Further, Flint discloses that "the current session key continues to be valid and only those files that are modified while the scanning is disabled have their session stamps invalidated" (Col. 7, lines 61-63 – emphasis added). In addition, Flint discloses that "[i]f a file is accessed (block 409) and the anti-virus scanning... has been stopped, the session stamp of the file is invalidated (block 415)" (Col. 8, line 67-Col. 9, line 4 – emphasis added), and that "when a file is accessed while the anti-virus scanning facility is inactive (block 411), the file can also be added to a rescan list in addition to having its session stamp invalidated at block 415" (Col. 9, lines 25-28).

However, Flint's disclosure that the program monitors relevant file system accesses while the scanning facility is stopped, where only those **files** that are **modified or accessed** while scanning is disabled have their session stamps invalidated, simply fails to even suggest a technique "wherein a user is allowed to disable the scanning module, and data is precluded from being transmitted from the storage to the central processing unit upon the disabling of the scanning module" (emphasis added), as claimed by appellant. Clearly, invalidating file session stamps for those files **accessed** or **modified** while the file scanning facility is stopped, as in Flint, fails to even suggest that "data is precluded from being transmitted from the storage to the central processing unit upon the disabling of the scanning module" (emphasis added), in the manner as claimed by appellant. To this end, Flint's disclosure of invalidating file session stamps for files modified or accessed while the scanning facility is stopped, simply fails to support the Examiner's allegation that the "above steps will be repeated as long as the virus scanner is off so the session stamp will never be validated and therefore the file cannot be accessed as further described with respect to figure 7 and column 10 lines 20-32."

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on appellant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above. A notice of allowance or a specific prior art showing of all of appellant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Group # 2: Claims 35-38

With respect to independent Claim 35, the Examiner has relied on Figure 15 item 413 of Makita to make a prior art showing of appellant's claimed "scanning module coupled to the central processing unit and the storage subsystem controller, the scanning module adapted for identifying the requests from the central processing unit, and scanning the data for malicious code in response to the requests."

Appellant respectfully asserts that item 413 of Figure 15 is a virus check unit to which "information to be recorded corresponding to the command is supplied" (see [0174] in Makita). Having information supplied to a virus check unit simply does not meet "scanning module adapted for identifying requests from the central processing unit" (emphasis added), as claimed by appellant.

In the Examiner's Answer mailed 01/29/2007, the Examiner has argued that '[a]ppellant first argues that supplying information to a virus check unit does not meet "a scanning module adapted for identifying requests from the central processing unit", however, in Makita the CPU of the host computer sends a command (i.e. request) fro access to a file (see paragraph 180), and the file is then accessed and scanned for viruses (see paragraphs 181 and 182).' Further, the Examiner has argued that "[t]herefore, the external storage unit (410 of figure 15) contains a system that receives and identifies requests for data, which is also scanned."

Appellant respectfully disagrees and asserts that Makita merely discloses that "the host computer 110 supplies a command to read out information from the recording medium 4 (step S8-1), [and that] information corresponding to the command is read out from the recording medium 4 (step S8-2)" (Paragraph 0180). Further, Makita discloses that "[t]he information read out from the recording medium 4 is supplied to the compression and expansion unit 411" where "[t]he information expanded in the compression and expansion unit 411 is supplied to the virus check unit 413" which "performs a virus check on the expanded information (step S8-4)" (Paragraphs 0181-0182).

However, the mere disclosure that the host computer supplies a command to read out information, which is then supplied to the compression and expansion unit, which in turn,

supplies expanded information to the virus check unit, as in Makita, simply fails to even suggest a "scanning module adapted for identifying requests from the central processing unit" (emphasis added), as claimed by appellant. Clearly, the expanded information from the compression and expansion unit being supplied to the virus check unit, as in Makita, simply fails to suggest that the "scanning module [is] adapted for identifying requests" (emphasis added), in the manner as claimed by appellant.

Further, the Examiner has relied on Makita's disclosed file management unit (Figure 15 item 211) and the following excerpts from Makita to make a prior art showing of appellant's claimed "event manager module coupled to the scanning module and the central processing unit, the event manager module adapted for receiving results of the scanning from the scanning module, the event manager module adapted to execute an event based on the results of the scanning":

> "The file management unit 121 manages the storage of files into, the readout and deletion of files from, and access rights o the recording medium 4 of the external storage 120. The file management unit 121 includes programs for managing the recording medium 4 formatted into a desired logical format in formats corresponding to operation systems such as 12-bit FAT (File Allocation Table) of MS-DOS, the 16-bit FAT of MS-DOS, and UNIX." [0091]
>
> "When a virus is discovered in step S8-5, a transmission to the host computer 110 is stopped, and the host computer 110 is notified that the virus is discovered (step S8-6)." [0183]

Appellant respectfully asserts that a file management unit that manages files, manages access to files, and manages the formatting of files along with stopping a transmission to the host computer when a virus is discovered as disclosed in Makita (see excerpts above) fails to meet "the event manager module adapted for receiving results of the scanning from the scanning module, the event manager module adapted to execute an event based on the results of the scanning" (emphasis added), as claimed by appellant. Simply nowhere in Makita is there any suggestion of an "event manager module" that is "adapted for receiving results of the scanning" and "adapted to execute an event based on the results of the scanning," as claimed.

In the Advisory Action dated 05/16/2005, the Examiner has relied on paragraph [0174] of Makita in arguing that the CPU in Makita sends a request to the scanning module to scan for

data. Thus, the Examiner has concluded that the scanning module must be adapted for identifying the requests from the CPU since it is adapted to receive requests for a data scan.

Appellant respectfully asserts that Makita merely teaches that "[w]hen a command to record information on the recording medium 4 is supplied from the host computer 110 (step S7-1), information to be recorded corresponding to the command is supplied to the virus check engine unit 413" (emphasis added). Thus, the virus check engine in Makita is not adapted for identifying requests, since no request is ever made by the host computer. In particular, the information in Makita is simply supplied to the virus check engine, and a request is not utilized. To emphasize, the host computer in Makita does not send a request to the scanner, but simply sends the information to the scanner. Thus, the scanner in Makita does not have a request to identify or respond to since it is only the information itself, which is being sent to the scanner and not a request.

In addition, in the Advisory Action dated 05/16/2005, the Examiner has relied on the file management unit as described in Makita paragraph [0091], in supporting the present rejection. However, appellant respectfully asserts that such file management unit simply manages "the storage of files into, the readout and deletion of files from, and access rights to the recording medium 4 of the external storage 120" ([0091]). Thus, the file management unit only manages files with respect to the recording medium.

In Makita, the only mention of scanning such files relates to scanning them when information is read out from the recording medium (see paragraph [0181]). Then, after the scanning, it is determined whether the file is transferred to a host computer (see paragraphs [0182]-[0184]). Since the file management unit only manages files with respect to the recording medium, such file management unit does not manage files with respect to their transmission from the virus check unit to the host computer. Therefore, clearly appellant's claimed "event manager module coupled to the scanning module and the central processing unit, the event manager module adapted for receiving results of the scanning from the scanning module, the event manager module adapted to execute an event based on the results of the scanning" has not been met by the Makita reference.

In the Examiner's Answer mailed 01/29/2007, the Examiner has argued that "[a]ppellant next argues that Makita fails to teach the modules adapted for receiving scanning results and executing an event based on the results." Further, the Examiner has argued that "[h]owever, as described in paragraphs 183 and 184 the data transmission is either stopped or allowed to continue to the host computer based on the results of the virus scanning," and "[t]herefore a portion of the external storage unit (410) receives the results and another portion causes an event to happen (stopping or allowing transmission to the host) based on those results."

Appellant respectfully disagrees and asserts that the excerpts from Makita relied upon by the Examiner merely disclose that "[w]hen a virus is discovered in step S8-5, a transmission to the host computer 110 is stopped, and the host computer 110 is notified that the virus is discovered (step S8-6)" (Paragraph 0183 – emphasis added). Further, Makita discloses that "[w]hen no virus is-discovered as a result of the virus check performed by the virus check unit 413, the expanded information is transmitted to the host computer 110 (step S8-7)" (Paragraph 0184).

However, merely disclosing that when a virus is discovered, the transmission to the host computer is stopped, and that the host computer is notified, as in Makita, simply fails to even suggest an "event manager module coupled to the scanning module and the central processing unit, the event manager module adapted for receiving results of the scanning from the scanning module, [and] the event manager module adapted to execute an event based on the results of the scanning" (emphasis added), as claimed by appellant. Clearly, generally disclosing that the transmission is stopped and the host is notified, as in Makita, simply fails to suggest an "event manager module adapted for receiving results of the scanning from the scanning module" or an "the event manager module adapted to execute an event based on the results of the scanning" (emphasis added), in the manner as claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above. A notice of allowance or a specific prior art showing of all of appellant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Group # 3: Claims 6 and 22

With respect to dependent Claim 6 et al., the Examiner has relied on Makita's paragraph [0213] to meet appellant's claimed technique "wherein the scanning module includes software." Appellant respectfully asserts that paragraph [0213] of Makita simply teaches that the "virus check can be performed even if a virus check program is not installed on the host computer." Thus, the only virus check software program disclosed in Makita relates to a virus checker on the host computer, and not that the scanning module (i.e. virus checker) includes software.

In the Examiner's Answer mailed 01/29/2007, the Examiner has argued that "all virus scanners are a combination of software and hardware for it to run on" and that "[f]urthermore, the combined references of Flint teaches a virus program (i.e. software) and this program is tired to a CPU and disk (see column 1 lines 36-50)."

Appellant respectfully disagrees and asserts that Flint merely discloses that "AV programs scan computer files for known viruses in a number of ways," and that "Virus scanning is, therefore, a resource intensive (CPU and disk I/O) and time-consuming task" (Col. 1, lines 36-45). However, merely disclosing that AV programs scan computer files for viruses and may be CPU and disk I/O intensive, as in Flint, simply fails to even suggest a technique "wherein the scanning module includes software" where "the scanning is performed by a scanning module coupled to a storage subsystem controller" (see independent Claim 1 – emphasis added), in the context as claimed by appellant. Clearly, AV programs that may be CPU and disk I/O intensive, as in Flint, simply fail to suggest that "the scanning module includes software" (emphasis added), in the manner as claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above. A notice of allowance or a specific prior art showing of all of appellant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Group # 4: Claims 7 and 23

With respect to dependent Claim 7 et al., the Examiner has relied on Figure 15 of Makita to meet appellant's claimed technique "wherein the scanning module includes hardware." Appellant respectfully asserts that Figure 15 merely shows that the virus check unit 413 is included in the external storage 4 (which may include logic stored on the external storage 4) and not that the virus check unit includes hardware itself.

In the Examiner's Answer mailed 01/29/2007, the Examiner has argued that "all virus scanners are a combination of software and hardware for it to run on" and that "[f]urthermore, the combined references of Flint teaches a virus program (i.e. software) and this program is tired to a CPU and disk (see column 1 lines 36-50)."

Appellant respectfully disagrees and asserts that Flint merely discloses that "AV programs scan computer files for known viruses in a number of ways," and that "Virus scanning is, therefore, a resource intensive (CPU and disk I/O) and time-consuming task" (Col. 1, lines 36-45). However, merely disclosing that AV programs scan computer files for viruses and may be CPU and disk I/O intensive, as in Flint, simply fails to even suggest a technique "wherein the scanning module includes hardware" where "the scanning is performed by a scanning module coupled to a storage subsystem controller" (see independent Claim 1 – emphasis added), in the context as claimed by appellant. Clearly, AV programs that may be CPU and disk I/O intensive, as in Flint, simply fail to suggest that "the scanning module includes hardware" (emphasis added), in the manner as claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above. A notice of allowance or a specific prior art showing of all of appellant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Group # 5: Claims 12 and 28

With respect to dependent Claim 12 et al., the Examiner has relied on paragraph [0183] of Makita to make a prior art showing of appellant's claimed technique "wherein the event includes disabling the scanning module in response to the event." Appellant respectfully asserts that the above cited reference from Makita merely teaches that "a transmission to the host computer 110 is stopped" ([0183]). Thus, there is simply no disclosure of any sort of "disabling [of] the scanning module" and especially not "in response to the event," as claimed by appellant.

In the Examiner's Answer mailed 01/29/2007, the Examiner has argued that "Makita teaches the disabling of functionality based on an event in paragraph 183 (the stopping of transmission based on the virus scanning results) and Flint teaches disabling a virus scanner based on user input (i.e. an event) (see column 9 lines 10-13)." Further, the Examiner has concluded that "[t]herefore the combination teaches disabling the scanning module in response to an event."

Appellant respectfully disagrees and asserts that Makita merely teaches that "[w]hen a virus is discovered in step S8-5, a transmission to the host computer 110 is stopped, and the host computer 110 is notified that the virus is discovered (step S8-6)." (Paragraph 0183 – emphasis added). However, the mere disclosure of stopping a transmission to a host computer when a virus is discovered, as in Makita, simply fails to even suggest a technique "wherein the event includes disabling the scanning module in response to the event" (emphasis added), as claimed by appellant. Clearly, stopping the transfer, as in Makita, fails to suggest "disabling the scanning module in response to the event" (emphasis added), in the manner as claimed by appellant.

Further, Flint discloses that "[i]f the user input specifies the termination of the anti-virus program (block 427), a termination process... is performed" (Col. 9, lines 10-13 – emphasis added). However, performing a termination process of the anti-virus program if the user input specifies termination, as in Flint, clearly fails to suggest a technique "wherein the event includes disabling the scanning module in response to the event" (emphasis added), as claimed by appellant. Cleary, user input specifying termination, as in Flint, fails to meet appellant's claimed "disabling the scanning module in response to the event" (emphasis added), in the manner as claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above. A notice of allowance or a specific prior art showing of all of appellant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Group # 6: Claims 14 and 30

With respect to dependent Claim 14 et al, the Examiner has relied on Makita's teaching of formatting the recording medium ([0053]-[0054]) to make a prior art showing of appellant's claimed technique "wherein the scanning includes content scanning." The Examiner has stated that content scanning is used to determine a format of the data and to format the data. However, Makita clearly only teaches formatting the recording medium (see specifically paragraph [0054]) and not providing content scanning of the requested data for malicious code, in the manner claimed by appellant.

In the Examiner's Answer mailed 01/29/2007, the Examiner has argued that "the virus check unit scans the requested file to check if the file contains any known viruses (scanning for content)" and "[t]herefore, Makita teaches content scanning."

Appellant respectfully disagrees and asserts that the excerpts from Makita relied upon by the Examiner merely teach "providing the file management unit included in an external storage with a formatting function of formatting a recording medium, it becomes unnecessary for the host computer to perform formatting" (Paragraph 0054 – emphasis added). However, providing the file management unit a formatting function for formatting a recording medium, as in Makita, in no way suggests a technique "wherein the scanning includes content scanning" (emphasis added), as claimed by appellant.

Furthermore, the Makita discloses that "the virus check unit 413 performs a virus check on the expanded information (step S8-4)" where "[i]t is determined whether a virus is discovered in the information" (Paragraph 182 – emphasis added). Clearly, the virus checker unit performing a virus check to determine if a virus is discovered in the information, as in Flint, simply fails to

suggest a technique "wherein the scanning includes content scanning" (emphasis added), in the manner as claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above. A notice of allowance or a specific prior art showing of all of appellant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Group # 7: Claim 40

With respect to dependent Claim 40, the Examiner has continued to rely on Flint's disclosed system where "[t]he user or administrator also faces the challenges inherent in maintaining the external database" (Col. 2, lines 19-20) to make a prior art showing of appellant's claimed technique "wherein the user includes a remote administrator."

Appellant respectfully asserts that Flint's basic mention of an administrator that maintains an external database does not meet appellant's "user [that] includes a remote administrator" (Claim 40) in the context of appellant's claim language, such that the "user is allowed to disable the scanning module" (see independent Claim 1).

In the Advisory Action dated 05/16/2005, the Examiner argued that Flint does not provide support for a user being an administrator, but that Flint discloses that a user or administrator can maintain a similar system to that of Makita's and appellant's. The Examiner then concludes by stating that "Flint provides support that a user can be an administrator."

Appellant respectfully asserts that the Examiner's arguments are not clear. First the Examiner states that Flint does not support a user being an administrator, and then the Examiner goes on to state that Flint does provide support that a user can be an administrator. Appellant again argues that the only administrator disclosed in Flint relates to an administrator who maintains a database, and not a remote administrator who can disable the scanning module, as claimed by appellant (see Claim 40 which depends from Claim 1).

In the Examiner's Answer mailed 01/29/2007, the Examiner has argued that "Flint teaches that a user can disable a virus scanner (see column 9 lines 10-13)" and "that the user can be an administrator (see column 2 lines 19-20)." Further, the Examiner has concluded that "when combined with the remote requests of Makita the combined references teach a remote administrator can disable the scanning module."

Appellant respectfully disagrees and asserts that excerpts from Flint relied upon by the Examiner merely disclose that "[t]he user **or** administrator also faces the challenges inherent in maintaining the external database" (Col. 2, lines 19-20), and that "[i]f the user input specifies the termination of the anti-virus program (block 427), a termination process... is performed" (Col. 9, lines 10-13 – emphasis added). However, the mere disclosure that a user or administrator may maintain an external database, and that they user may terminate the anti-virus program, as in Flint, simply fails to even suggest a technique "wherein the user includes a remote administrator" where "user is allowed to disable the scanning module" (see independent Claim 1 – emphasis added), in the context as claimed by appellant.

Furthermore, appellant respectfully asserts that Makita fails to support the Examiner's argument of remote requests, and instead, merely teaches "a storage device which is connected to a host computer and stores information processed in the host computer," and "an external storage connected to a host computer" (Abstract). Clearly, an external storage device connected to a host computer, as in Makita, simply fails to even suggest a technique "wherein the user includes a remote administrator" where "user is allowed to disable the scanning module" (see independent Claim 1 – emphasis added), in the context as claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above. A notice of allowance or a specific prior art showing of all of appellant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Issue # 3:

The Examiner has rejected Claim 41 under 35 U.S.C. 103(a) as being unpatentable over Makita, U.S. Patent No. 2001/0007120, in view of Flint, U.S. Patent No. 6,735,700, in further view of Browne, U.S. Patent No. 6,272,533.

Group # 1: Claim 41

With respect to dependent Claim 41, the Examiner has relied on Browne to make a prior art showing of appellant's claimed technique "wherein the user is allowed to disable the storage, and the data is precluded from being transmitted to the storage from the central processing unit upon the disabling of the storage." Specifically, the Examiner has stated that Browne discloses a secure computing system in which a manual switch can be pressed so that data is precluded from being written to a storage device.

Appellant respectfully asserts that Browne merely teaches the "disabling [of the] alteration of data residing on a mass storage device" (see Abstract). Thus, simply disabling the alteration of data, as in Browne, does not meet appellant's specifically claimed "disabling of the storage," let alone disabling the storage such that "data is precluded from being transmitted to the storage from the central processing unit upon the disabling of the storage."

In the Examiner's Answer mailed 01/29/2007, the Examiner has argued that 'Browne teaches the use of a read mode that is user activated (see column 4 lines 51-64) and when in read mode data cannot be written to the storage device (see column 8 lines 65-67 "read only").' Further, the Examiner has concluded that "[t]herefore, Browne discloses a user is allowed to disable the storage, and the data is precluded from being transmitted to the storage upon said disabling."

Appellant respectfully disagrees and asserts that Browne discloses that "[t]he storage device is responsive to the processor for selectively operating in a read mode of operation for reading previously stored data and in a write mode of operation for storing data" (see Col. 4, lines 54-57). Further, Browne discloses that "the status of each device is indicated by a tricolor LED 214... [such as] yellow [which indicates] that the corresponding device can be operated in a read only mode of operation (write-inhibited)" (see Col. 8, lines 65-67 – emphasis added).

However, appellant respectfully asserts that the storage device operating in a read only mode (write-inhibited), as in Browne, simply fails to suggest that the "user is allowed to disable the storage," much less a technique "wherein the user is allowed to disable the storage, and the data is precluded from being transmitted to the storage from the central processing unit upon the disabling of the storage" (emphasis added), as claimed by appellant. Clearly, operating the device in a read only mode, as in Browne, simply fails to even suggest "the disabling of the storage" (emphasis added), in the manner as claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above. A notice of allowance or a specific prior art showing of all of appellant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Group # 2: Claim 42

In the Examiner's Answer mailed 01/29/2007, the Examiner has presented new grounds of rejection, and has rejected Claim 42 under 35 U.S.C. 103(a) as being unpatentable over Makita, in view of Flint, and in further view of Browne. Specifically, the Examiner has relied upon Col. 9, lines 5-39 from Flint, and Col. 4, lines 61-64 from Browne to make a prior art showing of appellant's claimed technique "wherein it is determined whether the storage is disabled only after determining whether the scanning module is disabled."

Appellant respectfully disagrees, and asserts that the excerpt from Flint relied upon by the Examiner discloses that "[i]f the user input specifies the termination of the anti-virus program (block 427), a termination process... is performed" (Col. 9, lines 10-13 – emphasis added). Further, appellant asserts that the excerpt from Browne relied upon by the Examiner merely discloses that "the system further includes a second manually operative switch selectively disabling the storage device from operating in the write mode of operation" (Col 4, lines 61-64 – emphasis added).

However, the mere disclosure of a user specifying the termination of the anti-virus program, as in Flint, and the disclosure of a switch which selectively disables the write mode of operation of the storage device, as in Browne, simply fails to even suggest a technique "wherein it is determined whether the storage is disabled only after determining whether the scanning module is disabled" (emphasis added), as claimed by appellant. Clearly, Flint and Browne, as relied upon by the Examiner, simply fail to suggest "determin[ing] whether the storage is disabled only after determining whether the scanning module is disabled" (emphasis added), in the manner as claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above. A notice of allowance or a specific prior art showing of all of appellant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Group # 3: Claim 43

In the Examiner's Answer mailed 01/29/2007, the Examiner has presented new grounds of rejection, and has rejected Claim 43 under 35 U.S.C. 103(a) as being unpatentable over Makita, in view of Flint, and in further view of Browne. Specifically, the Examiner has relied upon Col. 9, lines 5-39 from Flint to make a prior art showing of appellant's claimed technique "wherein the disabling and enabling of the storage and the scanning module provides increased functionality in conditionally precluding transmission of the data to the storage from the central processing unit."

Appellant respectfully disagrees, and asserts that the excerpt from Browne relied upon by the Examiner merely discloses that "the system further includes a second manually operative switch selectively disabling the storage device from operating in the write mode of operation" (Col 4, lines 61-64 – emphasis added). However, the mere disclosure of selectively disabling the write mode of operation of the storage device, as in Browne, simply fails to even suggest a technique "wherein the disabling and enabling of the storage and the scanning module provides increased functionality in conditionally precluding transmission of the data to the storage from the central

processing unit" (emphasis added), as claimed by appellant. Clearly, disabling the write mode of operation of the storage device, as in Browne, fails to suggest "disabling and enabling of the storage and the scanning module" (emphasis added), in the manner as claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above. A notice of allowance or a specific prior art showing of all of appellant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Issue # 4:

In the Examiner's Answer mailed 01/29/2007, the Examiner has presented a new grounds of rejection, and has rejected Claims 17, 18, 20-23, 26-32, 34, and 39 under 35 U.S.C. 101 as being directed to non-statutory subject matter.

Group # 1: Claims 17, 18, 20-23, 26-32, and 34

In the Examiner's Answer mailed 01/29/2007, the Examiner has argued that "[t]he computer code products are merely computer code and the specification allows the means to be merely software, therefore these claims lack the necessary physical articles or objects to constitute a machine or a manufacture within the meaning of 35 USC 101," and "[a]s such, they fail to fall within a statutory category." Appellant respectfully disagrees and asserts that in Claims 17, and 34, appellant claims that "scanning is performed by a scanning module coupled to a storage subsystem controller" (emphasis added), as claimed, thus rendering appellant's claimed techniques statutory. Furthermore, dependent Claims 18, 20-23, 26-32 are statutory due to their dependence upon independent Claim 17.

Group # 2: Claim 39

In the Examiner's Answer mailed 01/29/2007, the Examiner has argued that "[t]he computer code products are merely computer code and the specification allows the means to be merely

software, therefore these claims lack the necessary physical articles or objects to constitute a machine or a manufacture within the meaning of 35 USC 101," and "[a]s such, they fail to fall within a statutory category." Appellant respectfully disagrees and asserts that in Claim 39, appellant claims "receiving results of the scanning from the scanning module, the event manager module adapted to execute an event" (emphasis added), as claimed, thus rendering appellant's claimed techniques statutory.

In view of the remarks set forth hereinabove, all of the independent claims are deemed allowable, along with any claims depending therefrom.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P020).

Respectfully submitted,

By: /KEVINZILKA/ Date: March 29, 2007

Kevin J. Zilka
Reg. No. 41,429

Zilka-Kotab, P.C.
P.O. Box 721120
San Jose, California 95172-1120
Telephone: (408) 971-2573
Facsimile: (408) 971-4660